UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,109	12/20/2001	Donald P. Matthews JR.	2875.0660001	7508

26111 7590 08/15/2006

STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/026,109	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are pending.

2. Amendment filed 06/28/2006 has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 5-9, 11-13, 17-21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews Jr. (hereinafter Matthews) in view of Hronik (US 20030167374).

As per claim 1, Matthews teaches a cryptography accelerator for generating a stream cipher, the cryptography accelerator comprising: a key stream generation core for performing key stream generation operations (Col. 2, lines 51-53; Col. 3, lines 1-3; Col. 7, lines 1-2); a memory associated with the key stream generation core, the memory including a plurality of input ports configured to obtain write data associated with a stream cipher

and a plurality of output ports configured to provide read data associated with the stream cipher, wherein the key stream generation core and the memory are operable for performing a plurality of read data operations associated with generating the stream cipher in a single cycle (Col. 2, lines 56-62; Col. 3, lines 4-6; Col. 4, lines 27-29,. Col. 7, lines 2-7).

Matthews does not explicitly disclose a memory for performing a plurality of write data operations in a single cycle.

Hronik in analogous ad, however, discloses a memory for performing a plurality of write data operations in a single cycle (Page 1, paragraph 14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include a memory for performing a plurality of write data operations in a single cycle. This modification would have been obvious because a person having ordinary skill in the ad would have been motivated to do so in order to provide a fast hardware implementation of encryption and decryption circuit by reducing the number of cycles needed to perform encryption/decryption which in turn greatly increases efficiency and reduces cost (Col. 2, lines 58-64; Matthews).

As per claims 5 and 17, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator wherein the stream cipher is associated with three variables (Col. 11, lines 38-39 and lines 59-61).

As per claims 6 and 18, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator wherein a read operation and a write operation are performed using a first variable and the memory in a first cycle (Col. 12, lines 22-25).

As per claims 7 and 19, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory wherein a read operation and a write operation are performed using a second variable and the memory in a second cycle (Col. 12, lines 26-27 and lines 38-42).

As per claims 8 and 20, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory wherein a read operation and a write operation are performed using a third variable and the memory in a third cycle (Col. 12, lines 43-57).

As per claim 9 and 21, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory wherein the stream cipher is ARCM (Col. 2, lines 2-4; Col. 7, lines 7-8; ARC4 is interpreted as RC4, the interpretation is given based on the description given of the disclosure).

As per claims 11 and 23, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory comprising a plurality of byte flops (Figure 8A, items 808, 810, 812).

As per claim 12, the combination of Matthews and Hronik teach all the subject matter as discussed above. In addition, Matthews further disclose a cryptographic accelerator wherein the key stream generation core is operable to perform key shuffle operations and key stream generation operations (Col. 2, lines 51-53; Col. 3, lines 1-3; Col. 7, lines 1-2; Col. 11, lines 54-57; Col. 12, lines 43-58).

As per claim 13, Matthews teaches a memory associated with a cryptography engine for generating a stream cipher, the memory comprising: a plurality of input ports configured to obtain write data associated with generating a stream cipher (Figure 6;

Col. 2, lines 56-62; Col. 3, lines 4-6; Col. 4, lines 27-29; Col. 7, lines 2-7); a plurality of output ports configured to provide read data associated with the stream cipher, wherein a plurality of read data operations associated with generating the stream cipher are performed in a single cycle (Figure 6; Col. 2, lines 56-62; Col. 3, lines 4-6; Col. 4, lines 27-29; Col. 7, lines 2-7).

Matthews does not explicitly disclose a memory for performing a plurality of write data operations in a single cycle.

Hronik in analogous art, however, discloses a memory for performing a plurality of write data operations in a single cycle (Page 1, paragraph 14). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include a memory for performing a plurality of write data operations in a single cycle. This modification would have been obvious because a person having ordinary skill in the ad would have been motivated to do so in order to provide a fast hardware implementation of encryption and decryption circuit by reducing the number of cycles needed to perform encryption/decryption which in turn greatly increases efficiency and reduces cost (Col. 2, lines 58-64; Matthews).

5. Claims 2-3 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Matthews and Hronik as applied to claims 1 and 13 above, and further in view of Kundarewich et al (hereinafter Kundarewich) Title "A CPLD-based RC4 cracking system" (Pages 397-402).

As per claims 2 and 14, the combination of Matthews and Hronik teach all the subject matter as discussed above. Both references do not explicitly disclose a cryptography accelerator wherein generation of the stream cipher is pipelined using coherency checking.

Kundarewich in analogous art however, disclose generation of the stream cipher that is pipelined using coherency checking (Page 398, col. 2, paragraph 2; …the order of the two writes is done to preserve the coherence of data…).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews and Hronik to include generation of the stream cipher that is pipelined using coherency checking. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Kundarewich (Page 398, paragraph 2) in order to perform read and write at the same clock cycle.

As per claims 3 and 15, the combination of Matthews and Hronik teach all the subject matter as discussed above. Both references do not explicitly disclose a cryptography accelerator wherein the coherency checking comprises determining whether a write address is the same as a read address in a single cycle.

Kundarewich in analogous ad however, disclose a coherency checking comprising determining whether a write address is the same as a read address in a single cycle (Page 398, col. 2, paragraphs 2 and 3; …CPLD supports only a single read or write access…an extra clock cycle is not necessary…).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews and Hronik to include a coherency checking comprising determining whether a write address is the same as a read address in a single cycle. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Kundarewich (Page 398, paragraph 2) in order to perform read and write at the same clock cycle.

6. Claims 4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Matthews, Hronik, and Kundarewich as applied to claims 3 and 15 above, and further in view of Correale Jr. (hereinafter Correale) (US 4998221).

As per claims 4 and 16, the combination of Matthews, Hronik and Kundarewich teach all the subject matter as discussed above. Neither of the references, however, explicitly discloses a cryptography accelerator wherein a read operation bypasses the memory when the write address is the same as the read address.

Correale in analogous art, however, disclose a read operation that bypasses the memory when the write address is the same as the read address (Col. 3, lines 8-28; Col. 4, lines 7-9).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews, Hronik and Kundarewich to include a read operation that bypasses the memory when the write address is the same as the read address. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Correale (Abstract) in order shorten the time required to perform a write and read operation.

7. Claims 10 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Matthews and Hronik as applied to claims 1 and 13 above, and further in view of Schneier ("Applied Cryptography" pages 397-398).

As per claims 10 and 22, the combination of Matthews and Hronik teach all the subject matter as discussed above. Both references do not explicitly disclose a cryptography accelerator wherein the memory is initialized in a single cycle.

Schneier in analogous art however, disclose a cryptographic accelerator wherein the memory is initialized in a single cycle (Page 397, line 23; …initializing the S-box and fill it linearly).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include a cryptographic accelerator wherein the memory is initialized in a single cycle. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Schneier (Page 397) in order to provide a faster encryption.

Response to Arguments

8. Applicant's arguments filed 06/28/2006 have been fully considered but they are not persuasive. Applicant argues there is no motivation to combine Hronik with Matthews because there is no explanation how one would overcome the dependencies

described in Applicant's specification and the further references combined fail to make up for this deficiency.

With respect to Applicant's argument that there is no motivation to combine Hronik with Matthews because there is no explanation how one would overcome the dependencies described in Applicant's specification, first Applicant's specification states, "One read **may be** dependent on a prior write, or a write **may be** dependent on another prior write. Because Of the dependencies, ARC4 operations are **typically** performed in a strict sequence" (emphasis added). Based on this reading of the specification there could be dependencies, but nowhere does it state there has to be any dependencies therefore there does not exist a need to overcome dependencies that only may exist. Therefore as taught by Matthews, providing a fast hardware implementation of encryption and decryption circuit by reducing the number of cycles needed to perform encryption/decryption which in turn greatly increases efficiency and reduces cost (Col. 2, lines 58-64; Matthews) would motivate one of ordinary skill in the art to perform a plurality of write data operations in a single cycle as taught by Hronik.

Applicant's argument that the further references combined fail to make up for this deficiency is moot in view of the above response.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Batcher (US

6873707 and US 7006634) discloses methods for accelerating the RC4 algorithm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER